

Implemetasi Jaringan Saraf Tiruan Untuk Mendeteksi Serangan DDoS Pada Forensik Jaringan

Muhammad Aziz¹, Rusydi Umar², Faizin Ridho³

Magister Teknik Informatika

Universitas Ahmad Dahlan Yogyakarta, Indonesia

moch.aziz@tif.uad.ac.id¹, rusydi.umar@tif.uad.ac.id², faizin1607048009@webmail.uad.ac.id³

Abstract

Network attacks that are often carried out including using Distributed Denial of Service (DDoS) have caused significant financial losses and require very large recovery costs to reach double. Activities that damage, interfere with, steal data, and anything that harms the system owner of a computer network is illegal and can be legally sanctioned in court. Network forensics mechanism to find criminals in order to be ensnared by law. Investigators usually use network monitoring systems such as Intrusion Detection System (IDS) for forensics purposes. The use of IDS allows the detection of errors or changes in traffic and new types of attacks because attacks are carried out using syn packages, where the syn protocol is considered legal because it is needed in the authentication process of communication between devices in the Internet network. Signature-based detection and notification systems are also not strong enough to be used as evidence in the trial. An analysis mechanism is needed to test the accuracy of DDoS attacks that have been detected by the intrusion detection system. Testing the accuracy of DDoS attacks can be done using the neural network classification method using statistical calculations. Based on the results of the analysis and testing carried out found an accuracy value of 95.23%. These results can be used to support and strengthen the evidence of findings in the trial.

Keywords: DDoS, IDS, network forensics, JST

1. PENDAHULUAN

Denial of Service (DoS) merupakan permasalahan keamanan jaringan yang sampai saat ini terus berkembang secara dinamis dan meningkat secara signifikan dimana serangan yang sering dilakukan dengan mengeksploitasi sistem yang berdampak pada integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi dan infrastruktur[1]. Serangan *Distributed Denial of Service (DDoS)* yang sering dilakukan yaitu dengan *Flooding*, *Syn Flooding*, *DNS-flood*, dan *UDP-flood*[2] hingga membuat perangkat sistem menjadi *overload*. Serangan yang dapat menyebabkan kerugian keuangan yang signifikan serta membutuhkan biaya penanggulangan yang sangat besar hingga mencapai dua kali lipat [3][4]. Kegiatan merusak, mengganggu, mencuri data, dan segala hal yang merugikan pemilik sistem pada jaringan komputer adalah suatu tindak ilegal dan dapat dijatuhkan sanksi secara hukum di pengadilan[5]. Diperlukan mekanisme *network forensics*[6] untuk menemukan pelaku kejahatan agar dapat dijerat hukum. *Network Forensics* adalah kegiatan untuk merekam dan menganalisis peristiwa yang terjadi dalam jaringan untuk menemukan sumber serangan dan peristiwa lainnya[7].

Pendeteksian serangan yang paling umum dilakukan yaitu dengan menggunakan *Intrusion Detection System (IDS)*[8] dengan memantau lalu lintas jaringan yang dilalui. Investigator biasanya memanfaatkan sistem monitoring jaringan seperti IDS untuk keperluan *forensics*, dimana analisis dilakukan dengan memanfaatkan *log*[9][10] IDS maupun sistem notifikasi serangan[7][11]. Penggunaan IDS berbasis *signature* memungkinkan terjadinya kesalahan deteksi akibat perubahan traffic dan jenis serangan baru[12][13]. Disisi lain, serangan dengan memanfaatkan aliran paket data yang memanfaatkan protokol *syn* merupakan sebuah paket jaringan yang bersifat legal, karena protokol *syn* mutlak diperlukan dalam proses autentikasi komunikasi antar perangkat dalam jaringan Internet. Biasanya, ketika protokol *syn* dimanfaatkan untuk meluncurkan serangan DDoS dengan cara *flooding* target, hal ini diperkuat dengan laporan Kaspersky dalam situs laman resminya menyatakan bahwa persentase serangan menggunakan protokol *syn* mencapai 57.3%[14]. Hal ini menyulitkan *Intrusion Detection System (IDS)* untuk mendeteksi serangan sebagai artefak abnormal dan berakibat

pada tingginya *false-rate alert* yang dibangkitkan oleh *Intrusion Detection System* (IDS). Sistem deteksi berbasis *signature* dan notifikasi[15] tidak cukup kuat untuk dijadikan sebagai alat bukti dalam persidangan. Diperlukan mekanisme analisis untuk menguji akurasi serangan DDoS yang telah terdeteksi oleh IDS. Teknik pembelajaran mesin, dengan memvalidasi data jaringan yang diberikan untuk mengklasifikasikan dengan pengamatan yang sah berdasarkan anomali, dapat digunakan dalam proses forensik Jaringan[16]. Serangan DDoS melalui jaringan komputer, khususnya *Local Area Network* (LAN) mampu dideteksi menggunakan teknik multiklasifikasi, yaitu dengan menggabungkan metode data mining untuk mendapatkan akurasi yang lebih baik[17]. Pemanfaatan metode Neural Network dalam menganalisis serangan DDoS mampu memberikan Hasil 99.6% berdasarkan Variasi Hidden Neural Netwok[18][19]. Analisis serupa juga dilakukan dengan metode Naïve Bayes[20] menggunakan data set KDD99 berhasil menemukan akurasi tertinggi sebesar 99.7837%.

Berdasarkan latar belakang di atas untuk menentukan akurasi serangan DDoS guna keperluan *forensic* jaringan maka metode yang diusulkan untuk menganalisis dan menguji serangan DDoS yang terdeteksi pada IDS dengan dataset pada Laboratorium Riset Magister Teknik Informatika Universitas Ahmad Dahlan (LRis-MTIUAD) menggunakan metode jaringan saraf tiruan (JST) berdasarkan perhitungan statistik[21]. Diharapkan hasil analisis juga dapat digunakan sebagai pengembangan sistem keamanan pada jaringan.

2. METODE PENELITIAN

Jaringan Syaraf Tiruan (JST) adalah model komputasi yang diilhami secara biologis disusun oleh berbagai elemen pemrosesan (neuron). *Neuron* terhubung dengan *coefficients* atau bobot yang membangun struktur jaringan saraf. JST memiliki elemen untuk memproses informasi, yaitu fungsi transfer, masukan berbobot, dan *output*[22]. Tahapan analisis dilakukan dengan tahapan sebagai berikut:

2.1. Traffic Collection Dataset

Traffic Collection merupakan tahapan mengumpulkan dataset normal dan serangan pada jaringan Laboratorium Riset Universitas Ahmad Dahlan (LRis-UAD) dalam format .Pcap seperti pada Gambar 1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=1 Ack=1 Win=1351 Len=0
2	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=1461 Ack=1 Win=1351 Len=0
3	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=2521 Ack=1 Win=1351 Len=0
4	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=4201 Ack=1 Win=1351 Len=0
5	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=5841 Ack=1 Win=1351 Len=0
6	0.000000	192.168.10.111	8.253.181.235	TCP	54	58750 → 58750 [ACK] Seq=1 Ack=7961 Win=5180 Len=0
7	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=7701 Ack=1 Win=1351 Len=0
8	0.000000	8.253.181.235	192.168.10.111	TCP	54	58750 → 58750 [ACK] Seq=8461 Ack=1 Win=1351 Len=0
9	0.000000	8.253.181.235	192.168.10.111	TCP	54	[TCP Previous segment not captured] 88 → 58750 [ACK]
10	0.000000	8.253.181.235	192.168.10.111	TCP	54	[TCP Previous segment not captured] 88 → 58750 [ACK]
11	0.000000	8.253.181.235	192.168.10.111	TCP	54	[TCP Previous segment not captured] 88 → 58750 [ACK]
12	0.000000	192.168.10.111	8.253.181.235	TCP	54	58750 → 88 [ACK] Seq=1 Ack=14221 Win=5180 Len=0
13	0.000000	192.168.10.111	8.253.181.235	TCP	54	[TCP Dup. ACK 1242] 58750 → 88 [ACK] Seq=1 Ack=14221
14	0.000000	192.168.10.111	8.253.181.235	TCP	54	[TCP Dup. ACK 1242] 58750 → 88 [ACK] Seq=1 Ack=14221
15	0.000000	8.253.181.235	192.168.10.111	HTTP	54	1514 Continuation
16	0.000000	8.253.181.235	192.168.10.111	HTTP	54	1514 Continuation

Gambar 1. Traffic collection dataset

2.2. PreProcessing Data

Konversi data dengan format .pcap menjadi format .csv perlu dilakukan untuk mempermudah melakukan pengolahan data dengan perangkat lunak spreadsheet seperti yang terjadi pada Gambar 2. sebagai berikut :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.30.254	192.168.30.1	IPv4	1534	Fragmented IP protocol (proto=UDP 17, offset=0, ID=1310) [Reassembled in #1]
2	0.000001	192.168.30.254	192.168.30.1	ICMP	80	ICMP segment of a reassembled PDU
3	0.000001	192.168.30.254	192.168.30.1	IPv4	1534	Fragmented IP protocol (proto=UDP 17, offset=0, ID=1310) [Reassembled in #1]
4	0.000001	192.168.30.254	192.168.30.1	ICMP	80	ICMP segment of a reassembled PDU
5	0.000001	192.168.30.254	192.168.30.1	IPv4	1534	Fragmented IP protocol (proto=UDP 17, offset=0, ID=1310) [Reassembled in #1]
6	0.000001	192.168.30.254	192.168.30.1	ICMP	80	ICMP segment of a reassembled PDU
7	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
8	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
9	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
10	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
11	0.000001	192.168.30.254	192.168.30.1	IPv4	1534	Fragmented IP protocol (proto=UDP 17, offset=0, ID=1310) [Reassembled in #1]
12	0.000001	192.168.30.254	192.168.30.1	ICMP	80	ICMP segment of a reassembled PDU
13	0.000001	192.168.30.254	192.168.30.1	IPv4	1534	Fragmented IP protocol (proto=UDP 17, offset=0, ID=1310) [Reassembled in #1]
14	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
15	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
16	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
17	0.000001	192.168.30.254	192.168.30.1	TCP	60	TCP segment of a reassembled PDU
18	0.000001	192.168.30.254	192.168.30.1	IPv4	1534	Fragmented IP protocol (proto=UDP 17, offset=0, ID=1310) [Reassembled in #1]

Gambar 2. Konversi format .pcap menjadi format .csv

2.3. Pengolahan Data

Pengolahan data dilakukan dengan menentukan *ekstrasi feature* berdasarkan perhitungan statistic [21][18]. Penjumlahan dilakukan berdasarkan *fixed moving average window* [23] dengan durasi 3000 detik dan jeda 5 detik. Proses kuantifikasi bertujuan untuk mencirikan karakteristik aktivitas jaringan dalam satu rentang waktu serta memudahkan proses pelatihan dan pengujian klasifikasi data dengan neural network.

Perhitungan statistik yang digunakan adalah :

- 1) Nilai rerata (*average*) panjang paket jaringan dalam satu frame waktu yang telah ditentukan.
- 2) Nilai jumlah keseluruhan paket jaringan dalam satu frame waktu yang telah ditentukan.
- 3) Nilai varians dari variabel jeda waktu kedatangan paket jaringan yang bersumber dari IP tertentu dalam satu frame waktu yang telah ditentukan. Nilai varians dihasilkan dari persamaan 1.

$$a. \text{ Variasi Waktu} = \sqrt{\frac{\sum(t - \bar{t})^2}{n}} \quad (1)$$

b. \bar{t} = waktu paket diterima
c. t = rata-rata waktu paket diterima

- 4) Nilai varians dari variabel panjang paket jaringan yang bersumber dari IP tertentu dalam satu frame waktu yang telah ditentukan. Nilai varians dihasilkan dari persamaan 2.

$$a. \text{ Variasi Waktu} = \sqrt{\frac{\sum(p - \bar{p})^2}{n}} \quad (2)$$

b. \bar{p} = panjang paket diterima
c. p = rata-rata panjang paket diterima

- 5) Nilai kecepatan paket dalam satu frame waktu yang telah ditentukan, yang dihitung dengan persamaan 3.

$$a. \text{ Kecepatan Paket} = np * \frac{1}{T.a \text{ akhir} - T.a} \quad (3)$$

b. Dengan np = jumlah paket
c. $T.a \text{ akhir}$ = waktu akhir paket diterima
d. $T.a \text{ awal}$ = waktu awal paket diterima

- 6) Nilai jumlah keseluruhan bit data dalam satu frame waktu yang telah ditentukan.
- 7) Pemodelan: Melaksanakan pembentukan stuktur neural network dengan satu hidden layer, dengan jumlah neuron sebanyak $2n+1$ dimana n adalah jumlah neuron input [18][24].

3. HASIL DAN PEMBAHASAN

3.1. Packet Extraction

Pemrosesan data menggunakan rumus statistik dilaksanakan dengan proses ekstrasi. Proses ekstrasi dilakukan dengan mengimport data dalam format .csv. ke dalam aplikasi matlab untuk diolah seperti yang terlihat pada Gambar 3 berikut.

No	Time	Source	Destination	Protocol	Length	Info	Variable#	Variable#	Variable#
1	0.00000	192.168.20.1	192.168.20.1	IPV4	1514	Fragment...	off=0	ID=214f1f...	
2	0.00000	01.203.17...	192.168.20.1	ICMP	5	ICMP seq...			
3	0.00000	192.168.20.1	192.168.20.1	IPV4	1514	Fragment...	off=0	ID=214f1f...	
4	0.00000	01.203.17...	192.168.20.1	ICMP	5	ICMP seq...			
5	0.01353	192.168.20.1	192.168.20.1	IPV4	1514	Fragment...	off=0	ID=214f1f...	
6	0.01354	01.203.17...	192.168.20.1	ICMP	5	ICMP seq...			
7	0.01354	192.168.20.1	192.168.20.1	IPV4	1514	Fragment...	off=0	ID=214f1f...	
8	0.01355	01.203.17...	192.168.20.1	ICMP	5	ICMP seq...			
9	0.01355	192.168.20.1	192.168.20.1	IPV4	1514	Fragment...	off=0	ID=214f1f...	
10	0.01355	01.203.17...	192.168.20.1	ICMP	5	ICMP seq...			
11	0.01355	192.168.20.1	192.168.20.1	IPV4	1514	Fragment...	off=0	ID=214f1f...	

Gambar 3. Import data log IDS

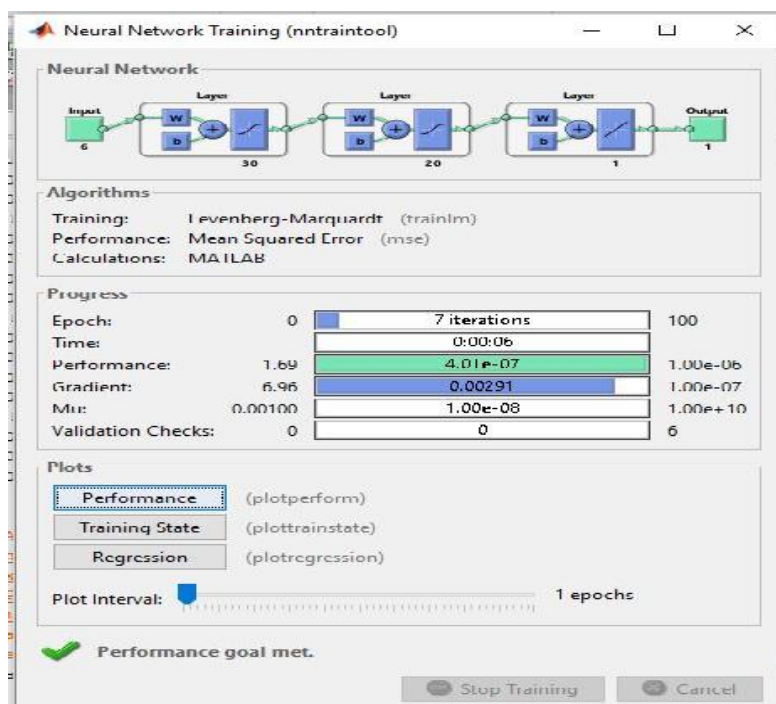
Dalam hal ini pengolahan dilakukan dengan melakukan pengelompokan setiap dataset dalam sebuah folder normal, DDoS dan data uji yang di load secara otomatis pada program matlab seperti yang terlihat pada Gambar 4. Proses klasifikasi data dilaksanakan dengan menggunakan dataset normal dengan jumlah data 60 file dan jumlah dataset serangan atau DDoS sebanyak 40 file.

Name	Date modified	Type	Size
data uji	23/03/2018 21:26	File folder	
normal	23/03/2018 21:26	File folder	
serangan	23/03/2018 21:26	File folder	
feature_normal	11/11/2017 11:01	MATLAB Data	1 KB
feature_serangan	11/11/2017 11:01	MATLAB Data	1 KB
feature_normal	33/03/2018 13:47	MATLAB Data	4 KB
IC	22/11/2017 13:12	MATLAB Code	8 KB
ICserang_load	11/11/2017 13:22	MATLAB Code	1 KB
net	25/9/2018 13:11	MATLAB Data	16 KB
parameter	25/9/2018 13:11	MATLAB Data	1 KB
Train	22/9/2018 17:20	MATLAB Figure	9 KB
Train	22/9/2018 17:20	MATLAB Code	23 KB
Uj	23/9/2018 22:21	MATLAB Figure	8 KB
Uj	25/9/2018 13:27	MATLAB Code	23 KB

Gambar 4. Lokasi file data latih dan data uji

3.2. Proses Pelatihan

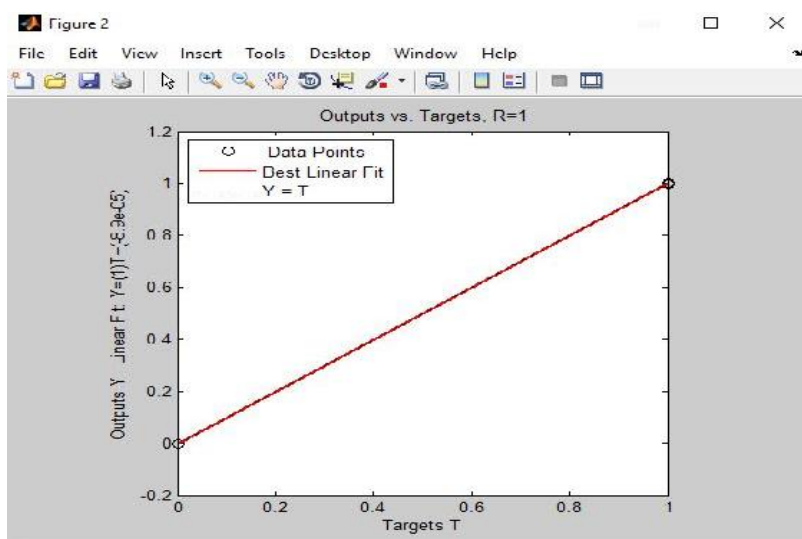
Pelatihan terhadap masing variasi arsitektur jaringan saraf tiruan dalam penelitian ini yaitu menggunakan fungsi Tansig, (Tangen Sigmoid), purelin (*Principal Components*) dan Trainln (*Levenberg-marquardt*). Tujuan dari variasi fungsi pelatihan yang memberikan akurasi tertinggi dalam mengenali trafik normal dan serangan. Pengolahan proses pelatihan dilakukan dengan menggunakan program matlab. Pelaksanaan pelatihan klasifikasi paket jaringan dari metode yang diterapkan menggunakan skema jumlah neuron (30-20-1) dengan Epoch 100 (iterasi) dan dengan nilai MSE sebesar 0.001 seperti yang tersaji pada Gambar 5.



Gambar 5. Proses pelatihan

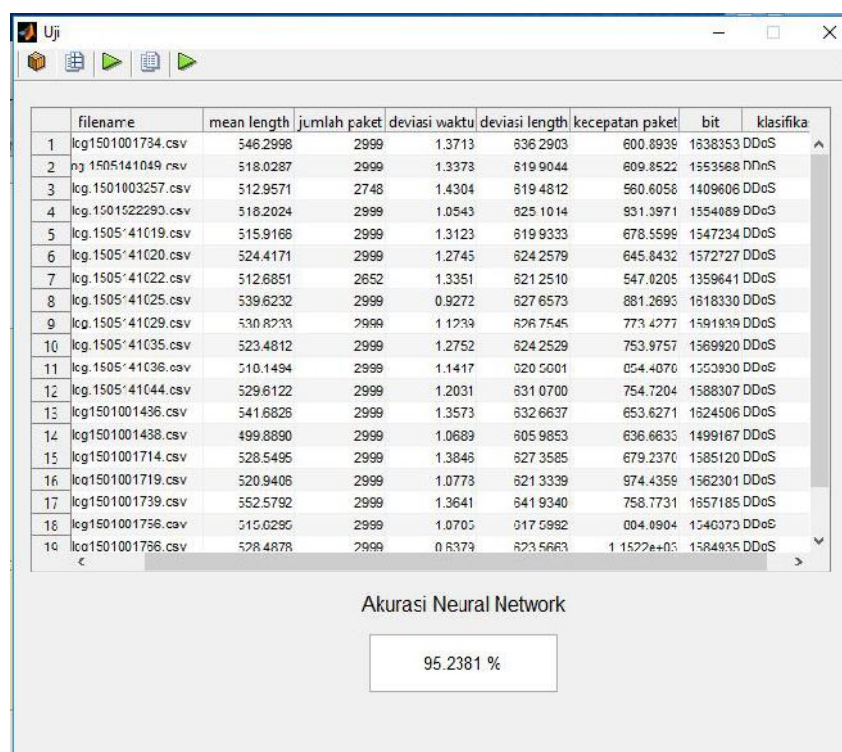
3.3. Hasil Analisis

Hasil pengujian yang dilakukan berdasarkan dataset Laboratorium Riset Universitas Ahmad Dahlan (LRis-UAD) menggunakan 60 data normal, 40 data DDoS dan 20 data uji menggunakan 6 input layer dengan Skema (30-20-1) menunjukkan performa nilai regresi R-test sebesar 1 yang berarti bahwa bobot-bobot koneksi antar neuron pada setiap *layer neural network* telah mampu memberikan hasil yang optimal dalam mengenali pola data input. Gambar 6 menunjukkan bahwa target berupa pasangan bilangan biner, yaitu 1-0 untuk kriteria trafik normal dan 0-1 untuk kriteria trafik DDoS, dengan input berupa trafik jaringan yang dihasilkan melalui proses normalisasi.



Gambar 6. Hasil pelatihan

Dalam hal ini pengujian dilakukan menggunakan data log IDS untuk menentukan akurasi berhasil di klasifikasi menggunakan metode jaringan saraf tiruan (JST). Hasil pengujian yang telah dilakukan menunjukkan bahwa log yang tersimpan pada sistem IDS terdeteksi sebagai serangan DDoS dengan nilai akurasi sebesar 95.23% seperti yang terdapat pada Gambar 7.



	filename	mean length	jumlah paket	deviasi waktu	deviasi length	kecepatan paket	bit	klasifikasi
1	log1501001734.csv	546.2988	2999	1.3713	836.2903	600.8939	1638353	DDoS
2	log1505141049.csv	518.0287	2999	1.3373	819.9044	609.8522	1553568	DDoS
3	log1501003257.csv	512.9571	2748	1.4304	819.4812	580.6058	1409606	DDoS
4	log1501522290.csv	518.2024	2999	1.0543	825.1014	831.3971	1554089	DDoS
5	log1505411019.csv	515.9168	2999	1.3123	819.9333	678.5599	1547234	DDoS
6	log1505411020.csv	524.4171	2999	1.2745	824.2579	645.8432	1572727	DDoS
7	log1505411022.csv	512.6851	2652	1.3351	821.2510	547.0205	1359641	DDoS
8	log1505411025.csv	539.6232	2999	0.9272	827.6573	881.2693	1618330	DDoS
9	log1505411029.csv	530.8233	2999	1.1233	826.7545	773.4277	1591939	DDoS
10	log1505411035.csv	523.4812	2999	1.2752	824.2529	753.9757	1569920	DDoS
11	log1505411036.csv	510.1494	2999	1.1417	820.5001	654.4070	1553930	DDoS
12	log1505411044.csv	529.6122	2999	1.2031	831.0700	754.7204	1588307	DDoS
13	log1501001436.csv	541.6825	2999	1.3573	832.6637	653.6271	1624506	DDoS
14	log1501001438.csv	499.8890	2999	1.0689	805.9853	636.6633	1499167	DDoS
15	log1501001714.csv	528.5495	2999	1.3846	827.3585	679.2370	1585120	DDoS
16	log1501001719.csv	520.9406	2999	1.0773	821.3339	974.4359	1562301	DDoS
17	log1501001739.csv	552.5792	2999	1.3641	841.9340	758.7731	1657185	DDoS
18	log1501001756.csv	515.0285	2999	1.0705	817.5992	604.0904	1546373	DDoS
19	log1501001756.csv	528.4878	2999	0.6373	823.5663	1.1522e+03	1584935	DDoS

Akurasi Neural Network

95.2381 %

Gambar 7. Hasil analisis menggunakan jaringan saraf tiruan

4. KESIMPULAN

Berdasarkan hasil analisis yang dilakukan disimpulkan bahwa informasi serangan yang telah dideteksi oleh IDS yang berbasis signatur perlu ditinjau kembali akurasinya menggunakan klasifikasi dengan perhitungan statistik. Berdasarkan analisis dan pengujian yang dilakukan dengan metode jaringan saraf tiruan, ditemukan hasil akurasi sebesar 95.2381%. Metode jaringan saraf tiruan dapat diterapkan dibidang forensik jaringan dalam menentukan hasil yang akurat dan membantu memperkuat bukti pada persidangan.

BAHAN REFERENSI

- [1] A. W. Muhammad and I. Riadi, 2017, "Deteksi Serangan DDoS Menggunakan Neural Network dengan Fungsi Fixed Moving Average Window," vol. 1, no. 3, pp. 115–122.
- [2] O. Blockbuster and R. Sony, 2016, "Threat Report,"
- [3] S. Geges and W. Wibisono, 2015, "Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle," *JUTI J. Ilm. Teknol. Inf.*, vol. 13, no. 1, pp. 53–67.
- [4] Es. Planet, "Intranet: DDoS attack growing but how much." [Online]. Available: <http://www.esecurityplanet.com/networksecurity/ddosattacks-growing-but-how-much.html>.
- [5] A. Fadlil, I. Riadi, S. Aji, and U. A. Dahlan, 2017, "Pengembangan sistem pengaman jaringan komputer berdasarkan analisis forensik jaringan," vol. 3, no. 1, pp. 11–18.
- [6] R. Messier, 2017, "Introduction to Network Forensics".
- [7] J. Fahana, R. Umar, and F. Ridho, 2017, "Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan," *Query J. Inf. Syst.*, vol. 1, no. 2, pp. 6–14.
- [8] G. Wang, 2017, "Neural Network Based Web Log Analysis for Web Intrusion Detection," *IEICE Trans. Inf. Syst.*, vol. E100D, no. 10, pp. 2265–2266.
- [9] F. Ridho, A. Yudhana, and I. Riadi, 2017, "Implementasi Log Dalam Forensik Router Terhadap Serangan Distributed Denial of Service (DDoS)," vol. VI, no. 2, pp. 15–21.
- [10] A. Iswardani and I. Riadi, 2016, "Denial of service log analysis using density k-means method,"

- J. Theor. Appl. Inf. Technol.*, vol. 83, no. 2, p. 2.
- [11] Fadhila Nisya Tanjung, Muhammad Irwan Padli Nasution, 2012, "Implementasi Pemrograman Java Untuk Alert Intrusion Detection System", pematang siantar, 31 agustus – 2 september 2012, ISBN 978-602-18749-0-5, <https://www.researchgate.net/publication/307973619> diakses 29 September 2016
 - [12] J. Ryan, M. J. Lin, and R. Miikkulainen, 1998, "Intrusion Detection with Neural Networks," *Proc. 1997 Conf. Adv. Neural Inf. Process. Syst. 10*, pp. 943–949.
 - [13] C. Fachkha and M. Debbabi, 2016, "Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization", vol. 18, no. 2.
 - [14] E. B. Alexander Khalimonenko, Oleg Kupreev, "ddos-report-in-q1-2018," *Securelist*. [Online]. Available: <https://securelist.com/ddos-report-in-q1-2018/85373/>.
 - [15] "pemanfaatan telegram keperluan forensik.pdf."
 - [16] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, 2017, "Towards Developing Network forensic mechanism for Botnet Activities in the IoT based on Machine Learning Techniques," *arXiv Prepr.*
 - [17] A. Fadlil, I. Riadi, and S. Aji, 2017, "DDoS Attacks Classification using Numeric Attribute-based Gaussian Naive Bayes," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 8, pp. 42–50.
 - [18] I. Riadi, A. W. Muhammad, and Sunardi, 2017, "Neural network-based ddos detection regarding hidden layer variation," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 15, pp. 3684–3691.
 - [19] I. Riadi and A. W. Muhammad, 2017, "Network Packet Classification using Neural Network based on Training Function and Hidden Layer Neuron Number Variation," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 248–252.
 - [20] V. D. Katkar and S. V. Kulkarni, 2013, "Experiments on detection of Denial of Service attacks using ensemble of classifiers," *2013 Int. Conf. Green Comput. Commun. Conserv. Energy*, vol. 2, no. 1, pp. 837–842.
 - [21] M. Chambali, A. W. Muhammad, and Harsono, 2018, "Classification of Network Packages Based on Statistical Analysis and Neural Network," *J. Pengemb. IT*, vol. 03, no. 1, pp. 67–70.
 - [22] S. Haykin, 2008, "Neural Networks and Learning Machines", vol. 3.
 - [23] S.-H.-A. ALI, N. FURUTANI, S. OZAWA, J. NAKAZATO, T. BAN, and J. SHIMAMURA, 2015, "Distributed Denial of Service (DDoS) Backscatter Detection System Using Resource Allocating Network with Data Selection," *Mem. Grad. Sch. Eng. Syst. Informatics Kobe Univ.*, no. 7, pp. 8–13.
 - [24] T. Zhao, D. C. T. Lo, and K. Qian, 2015, "A neural-network based DDoS detection system using hadoop and HBase," *Proc. - 2015 IEEE 17th Int. Conf. High Perform. Comput. Commun. 2015 IEEE 7th Int. Symp. Cybersp. Saf. Secur. 2015 IEEE 12th Int. Conf. Embed. Softw. Syst. H*, pp. 1326–1331.
 - [25] Nasution, Muhammad Irwan Padli, 2008, "Urgensi Keamanan Pada Sistem Informasi", *Jurnal Iqra' Volume 02 Nomor 02*.
 - [26] Nasution, MIP; Suendri; Samsudin; Zufria, I; Triase; Fakhriza, M; Ikhwan, A; 2018, "Biometrics for e-money transaction" ,AIP Conference Proceedings,2030,1,020301,2018,AIP Publishing